IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

FINTIV, INC.,	§	**Civil Action No.: 6:18-CV-372-ADA**
Plaintiff,	§	**JURY TRIAL DEMANDED**
v.	§	
APPLE INC.,	§	
Defendant.	§	

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Fintiv, Inc. ("Fintiv"), by and through its attorneys, for its First Amended Complaint against Defendant Apple Inc. ("Apple"), hereby alleges the following:

I. NATURE OF THE ACTION

1. This is a patent infringement action to end Defendant's unauthorized and infringing manufacture, use, sale, offering for sale, and/or importation of methods and products incorporating Plaintiff's patented inventions.

2. Fintiv is the owner of all right, title, and interest in and to United States Patent No. 8,843,125 (the "'125 Patent"), issued September 23, 2014 and titled "System and Method for Managing Mobile Wallet and its Related Credentials." A true and correct copy of the '125 Patent is attached hereto as Exhibit A.

3. Apple manufactures, provides, sells, offers for sale, imports, and/or distributes products and services which directly infringe the '125 Patent. Further, Apple indirectly infringes

the '125 Patent by inducing and/or contributing to infringement by others, including Apple device users, card issuers, and card issuer's authorized service providers.

4. Fintiv seeks monetary damages and prejudgment interest for Defendant's past and continuing infringement of the '125 Patent.

II. PARTIES

5. Plaintiff Fintiv, Inc. is a Delaware corporation having a principal place of business at 801 Barton Springs, Austin, Texas 78704. Fintiv is a corporation in good standing in the State of Delaware. A true and correct copy of the Certificate of Good Standing issued by Delaware's Secretary of State is attached hereto as Exhibit B.

6. Defendant Apple Inc. is a corporation organized and existing under the laws of California and has a regular and established places of business at 12535 Riata Vista Circle and 5501 West Parmer Lane, Austin, Texas. Apple employs thousands of people, including hundreds of engineers, who work at these locations in Texas. The work done at these Apple locations in Texas includes work related to Apple's iPhones and Apple Watch products. Apple can electronically access documents at its facilities in California and elsewhere from these locations in Austin, Texas, as found, inter alia, in *e-Watch Inc. v. Apple Inc.*, No. 2:13-CV-01061-JRG-RSP, 2016 WL 7338342, at *2 (E.D. Tex. Dec. 19, 2016) and *TracBeam, LLC v. Apple Inc.*, No. 6:14-CV-680, 2015 WL 5786449 (E.D. Tex. Sept. 29, 2015).

7. Apple also operates brick-and-mortar Apple Stores at Barton Creek Square, Austin, Texas and at Apple Domain Northside, Austin, Texas. *See* www.apple.com/retail/. Apple uses, offers for sale and sells iPhones and Apple Watch products that include Apple's Wallet functionality at these Apple Stores. Apple may be served with process through its registered agent for service in Texas: CT Corporation System, 1999 Bryant Street, Suite 900, Dallas, Texas 75201.

III. JURISDICTION AND VENUE

8. This is an action for patent infringement, which arises under the Patent Laws of the United States, in particular, 35 U.S.C. §§ 271, 281, 282, 284, and 285. The Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

9. This Court has personal jurisdiction over Apple because it has committed acts giving rise to this action within Texas and within this judicial district. Defendant also regularly does business or solicits business in this District and in Texas, engages in other persistent courses of conduct and derives substantial revenue from products and/or services provided in this District and in Texas, and has purposefully established substantial, systematic, and continuous contacts within this District and should reasonably expect to be sued in a court in this District. For example, Apple has offices in this District and has a Texas registered agent for service. Apple operates a website that solicits sales of the infringing products by consumers in this District and in Texas, has entered into partnerships with numerous resellers and distributors to sell and offer for sale the infringing products to consumers in this District and in Texas, both online and in stores, and offers support service to customers in this District and Texas. Given these contacts, the Court's exercise of jurisdiction over Apple will not offend traditional notions of fair play and substantial justice.

10. Venue in the Western District of Texas is proper pursuant to 28 U.S.C. §§ 1391(b), (c) and l400(b) because Apple has an established place of business in this District, including at 12535 Riata Vista Circle and 5501 West Parmer Lane, Austin, Texas, has committed acts within this judicial district giving rise to this action, and Apple continues to conduct business in this judicial district, including one or more acts of making, selling, using, importing and/or offering for sale infringing products or providing support service to Apple's customers in this District.

IV. THE PATENT-IN-SUIT

11. The '125 Patent relates to management of virtual cards stored on mobile devices and discloses provisioning a contactless card in a mobile device with a mobile wallet application.

12. The specification of the '125 Patent identifies technical problems in the prior art and claims improvement to these problems. For instance, the specification explains that prior art lacked "an effective means to manage various payment applets residing within the mobile device." ('125 Patent at 1:63-67.) Moreover, prior art implementations did not enable a user to "view any account specific information stored within the SE [Secure Element] or manage such applications with or without the use of POS [Point of Sale] equipment." *Id*. at 2:19-29. The specification further explains that "[a]nother limitation of current mobile wallet applications is the lack of support providing for such technology. . . . Accordingly, users may often be bombarded with various applications that may be inapplicable to the user, making the process more difficult than necessary." *Id*. at 2:30-44. Finally, the prior art did not allow for an easy way to update information: "As various service providers operate independently from one another, when an update is required by a particular service provider, each individual application is typically updated separately." *Id*. at 2:45-52. In essence, the '125 Patent claims a technical solution to these problems through a mobile wallet application and mobile wallet management system to store contactless cards in a secure element. The claimed technical solution is further incorporated in at least claims 11, 18, and 23 of the '125 patent.

13. Fintiv owns all substantial and material rights to and interests in the '125 Patent, including the right to recover damages for all past and future infringement thereof.

14. The '125 Patent is valid and enforceable.

COUNT I: DIRECT INFRINGEMENT OF THE '125 PATENT

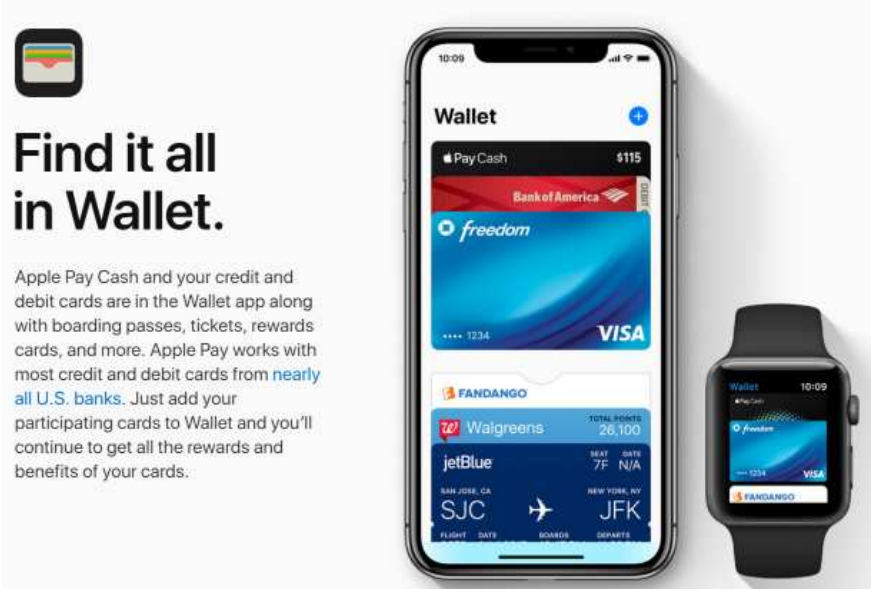
15. Fintiv incorporates paragraphs 1 through 15 herein by reference.

16. Apple, without authorization or license from Fintiv, has been and is presently directly infringing at least claim 11, 18, and 23 of the '125 Patent, as infringement is defined by 35 U.S.C. § 271(a), including through making, using (including for testing purposes), selling, offering for sale, and/or importing infringing products. Apple is thus liable for direct infringement of the '125 Patent pursuant to 35 U.S.C. § 271(a). Exemplary infringing products include Apple iPhone devices (including, at least, iPhone 6, 6 Plus, 6s, 6s Plus, SE, 7, 7 Plus, 8, 8 Plus, X, XR, XS, XS Max), Apple Watch devices (including, at least, Series 1, Series 2, Series 3, and Series 4), and the Apple Wallet Application (collectively, "the Apple Devices").

17. Claim 11, for example, recites:

> A method for provisioning a contactless card applet in a mobile device comprising a mobile wallet application, the method comprising:
>
> activating the mobile wallet application;
>
> connecting to a Trusted Service Manager (TSM) system;
>
> synchronizing the mobile wallet application with the TSM system;
>
> displaying a contactless card applet based on attributes of the mobile device;
>
> receiving a selection of a contactless card applet;
>
> retrieving a widget and a wallet management applet (WMA) corresponding to the contactless card applet; and
>
> provisioning the selected contactless card applet, the widget, and the WMA.

18. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to provision a contactless card in a mobile device that includes a mobile wallet application. All of this functionality is disclosed in at least claim 11 of the '125 patent.



https://www.apple.com/apple-pay/ (last visited on 11/6/2018).

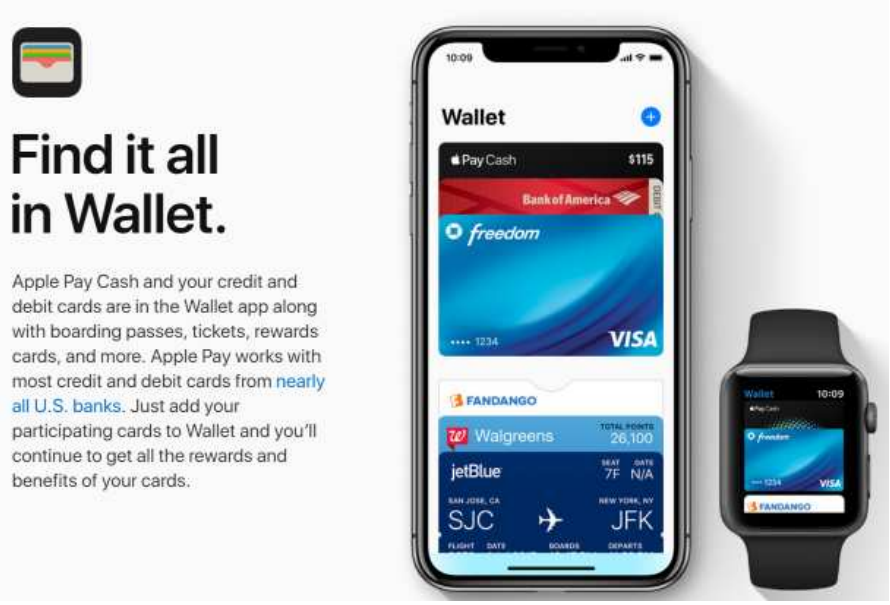
Wallet: Wallet is used to add and manage credit, debit, and store cards and to make payments with Apple Pay. Users can view their cards and may be able to view additional information provided by their card issuer, such as their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in:

- Setup Assistant and Settings for iOS
- The Watch app for Apple Watch
- The Wallet & Apple Pay system preference pane for Mac.

In addition, Wallet allows users to add and manage transit cards, rewards cards, boarding passes, tickets, gift cards, student ID cards, and more.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 47 (last visited 11/6/2018).

19. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to activate a mobile wallet application. All of this functionality is disclosed in at least claim 11 of the '125 patent.



https://www.apple.com/apple-pay/ (last accessed on 11/6/2018).

Wallet: Wallet is used to add and manage credit, debit, and store cards and to make payments with Apple Pay. Users can view their cards and may be able to view additional information provided by their card issuer, such as their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in:

- Setup Assistant and Settings for iOS
- The Watch app for Apple Watch
- The Wallet & Apple Pay system preference pane for Mac.

In addition, Wallet allows users to add and manage transit cards, rewards cards, boarding passes, tickets, gift cards, student ID cards, and more.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 47 (last visited 11/6/2018).

20. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to connect to a Trusted Service Manager (TSM) system. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

When you add credit, debit, prepaid, or transit cards

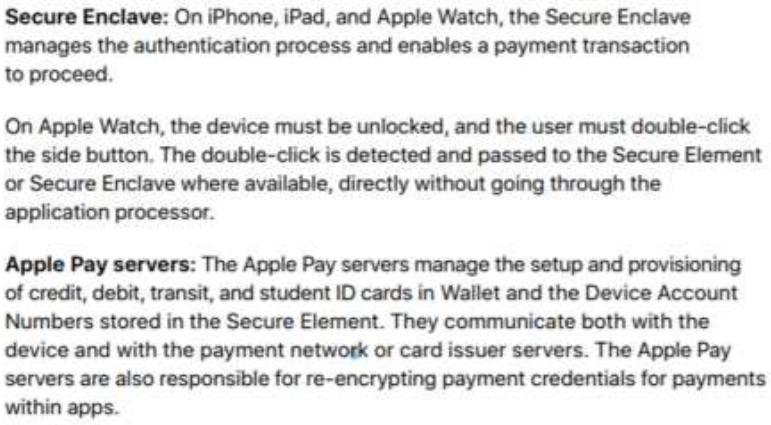
When you add a credit, debit, prepaid, or transit card (where available) to Apple Pay, information that you enter on your device is encrypted and sent to Apple servers. If you use the camera to enter the card information, the information is never saved on your device or photo library.

Apple decrypts the data, determines your card's payment network, and re-encrypts the data with a key that only your payment network (or any providers authorized by your card issuer for provisioning and token services) can unlock.

Information that you provide about your card, whether certain device settings are enabled, and device use patterns—such as the percent of time the device is in motion and the approximate number of calls you make per week—may be sent to Apple to determine your eligibility to enable Apple Pay. Information may also be provided by Apple to your card issuer, payment network, or any providers authorized by your card issuer to enable Apple Pay, to determine the eligibility of your card, to set up your card with Apple Pay, and to prevent fraud.

After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud.

https://support.apple.com/en-us/HT203027 (last accessed on 9/5/2018).



Secure Enclave: On iPhone, iPad, and Apple Watch, the Secure Enclave manages the authentication process and enables a payment transaction to proceed.

On Apple Watch, the device must be unlocked, and the user must double-click the side button. The double-click is detected and passed to the Secure Element or Secure Enclave where available, directly without going through the application processor.

Apple Pay servers: The Apple Pay servers manage the setup and provisioning of credit, debit, transit, and student ID cards in Wallet and the Device Account Numbers stored in the Secure Element. They communicate both with the device and with the payment network or card issuer servers. The Apple Pay servers are also responsible for re-encrypting payment credentials for payments within apps.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 47 (last visited 11/6/2018).

Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Wallet.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Wallet. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

When credit, debit, or prepaid cards (including store cards) are added, they will appear in a list of cards during setup assistant on devices that are signed in to the same iCloud account. These cards remain in this list for as long as they are active on at least one device. Cards are removed from this list after they have been removed from all devices for seven days. This feature requires two-factor authentication to be enabled on the respective iCloud account.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 48-49 (last visited 11/6/2018).

21. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to synchronize the mobile wallet application with the TSM system. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

When you add credit, debit, prepaid, or transit cards

When you add a credit, debit, prepaid, or transit card (where available) to Apple Pay, information that you enter on your device is encrypted and sent to Apple servers. If you use the camera to enter the card information, the information is never saved on your device or photo library.

Apple decrypts the data, determines your card's payment network, and re-encrypts the data with a key that only your payment network (or any providers authorized by your card issuer for provisioning and token services) can unlock.

Information that you provide about your card, whether certain device settings are enabled, and device use patterns—such as the percent of time the device is in motion and the approximate number of calls you make per week—may be sent to Apple to determine your eligibility to enable Apple Pay. Information may also be provided by Apple to your card issuer, payment network, or any providers authorized by your card issuer to enable Apple Pay, to determine the eligibility of your card, to set up your card with Apple Pay, and to prevent fraud.

After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud.

https://support.apple.com/en-us/HT203027 (last accessed on 9/5/2018).

Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Wallet.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Wallet. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

When credit, debit, or prepaid cards (including store cards) are added, they will appear in a list of cards during setup assistant on devices that are signed in to the same iCloud account. These cards remain in this list for as long as they are active on at least one device. Cards are removed from this list after they have been removed from all devices for seven days. This feature requires two-factor authentication to be enabled on the respective iCloud account.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 48-49 (last visited 11/6/2018).

Adding a credit or debit card manually to Apple Pay

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the camera on the device. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 49 (last visited 11/6/2018).

22. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to display a contactless card applet based on attributes of the mobile device. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

Wallet: Wallet is used to add and manage credit, debit, and store cards and to make payments with Apple Pay. Users can view their cards and may be able to view additional information provided by their card issuer, such as their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in:

- Setup Assistant and Settings for iOS
- The Watch app for Apple Watch
- The Wallet & Apple Pay system preference pane for Mac.

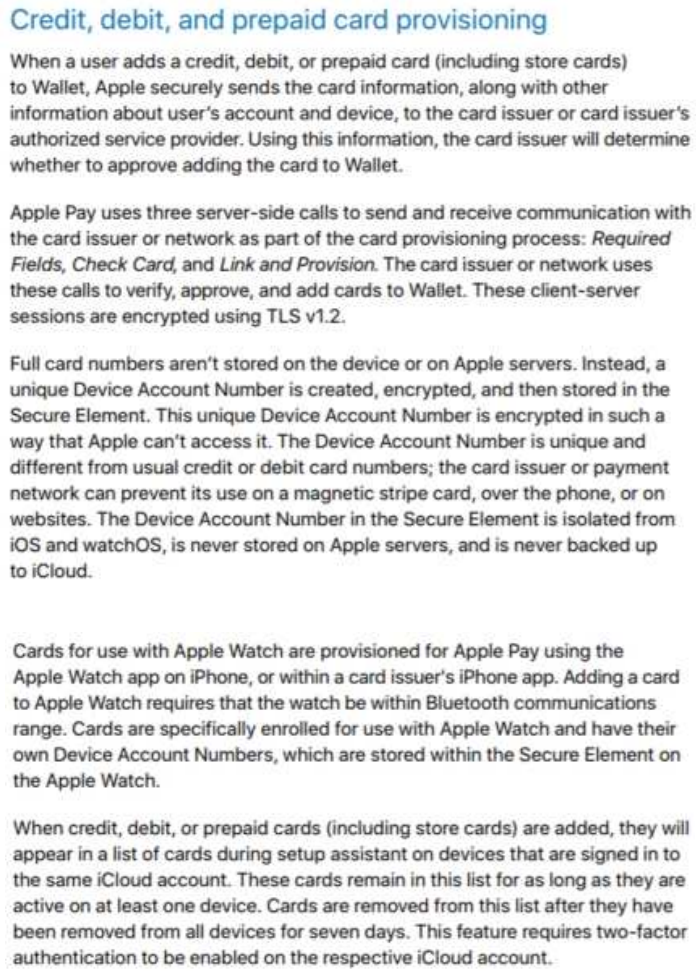
In addition, Wallet allows users to add and manage transit cards, rewards cards, boarding passes, tickets, gift cards, student ID cards, and more.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 47 (last visited 11/6/2018).

How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 48 (last visited 11/6/2018).



Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Wallet.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Wallet. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

When credit, debit, or prepaid cards (including store cards) are added, they will appear in a list of cards during setup assistant on devices that are signed in to the same iCloud account. These cards remain in this list for as long as they are active on at least one device. Cards are removed from this list after they have been removed from all devices for seven days. This feature requires two-factor authentication to be enabled on the respective iCloud account.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 48-49 (last visited 11/6/2018).

23. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to receive a selection of a contactless card applet. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

When you add credit, debit, prepaid, or transit cards

When you add a credit, debit, prepaid, or transit card (where available) to Apple Pay, information that you enter on your device is encrypted and sent to Apple servers. If you use the camera to enter the card information, the information is never saved on your device or photo library.

Apple decrypts the data, determines your card's payment network, and re-encrypts the data with a key that only your payment network (or any providers authorized by your card issuer for provisioning and token services) can unlock.

Information that you provide about your card, whether certain device settings are enabled, and device use patterns—such as the percent of time the device is in motion and the approximate number of calls you make per week—may be sent to Apple to determine your eligibility to enable Apple Pay. Information may also be provided by Apple to your card issuer, payment network, or any providers authorized by your card issuer to enable Apple Pay, to determine the eligibility of your card, to set up your card with Apple Pay, and to prevent fraud.

After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud.

https://support.apple.com/en-us/HT203027 (last accessed on 9/5/2018).

Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Wallet.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Wallet. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

When credit, debit, or prepaid cards (including store cards) are added, they will appear in a list of cards during setup assistant on devices that are signed in to the same iCloud account. These cards remain in this list for as long as they are active on at least one device. Cards are removed from this list after they have been removed from all devices for seven days. This feature requires two-factor authentication to be enabled on the respective iCloud account.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 48-49 (last visited 11/6/2018).

Adding a credit or debit card manually to Apple Pay

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the camera on the device. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 49 (last visited 11/6/2018).

24. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to retrieve a widget and a wallet management applet (WMA) corresponding to the contactless card applet. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

Adding a credit or debit card manually to Apple Pay

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the camera on the device. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

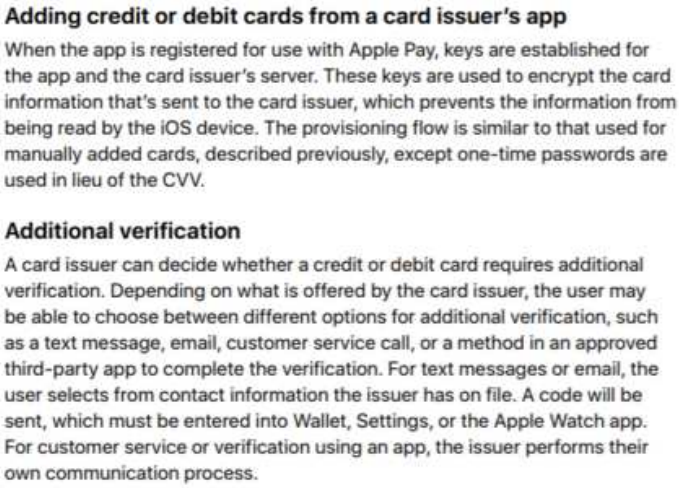
If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 49 (last visited 11/6/2018).



Adding credit or debit cards from a card issuer's app

When the app is registered for use with Apple Pay, keys are established for the app and the card issuer's server. These keys are used to encrypt the card information that's sent to the card issuer, which prevents the information from being read by the iOS device. The provisioning flow is similar to that used for manually added cards, described previously, except one-time passwords are used in lieu of the CVV.

Additional verification

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, customer service call, or a method in an approved third-party app to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which must be entered into Wallet, Settings, or the Apple Watch app. For customer service or verification using an app, the issuer performs their own communication process.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 50 (last visited 11/6/2018).

25. As reflected in Apple's own product literature illustrated below, the Apple Devices are enabled to provision the selected contactless card applet, the widget, and the WMA. All of this functionality is disclosed in at least claim 11 of the '125 Patent.

Adding a credit or debit card manually to Apple Pay

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the camera on the device. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 49 (last visited 11/6/2018).

Adding credit or debit cards from a card issuer's app

When the app is registered for use with Apple Pay, keys are established for the app and the card issuer's server. These keys are used to encrypt the card information that's sent to the card issuer, which prevents the information from being read by the iOS device. The provisioning flow is similar to that used for manually added cards, described previously, except one-time passwords are used in lieu of the CVV.

Additional verification

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, customer service call, or a method in an approved third-party app to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which must be entered into Wallet, Settings, or the Apple Watch app. For customer service or verification using an app, the issuer performs their own communication process.

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf at p. 50 (last visited 11/6/2018).

COUNT II: INDIRECT INFRINGEMENT OF THE '125 PATENT

26. Fintiv incorporates paragraphs 1 through 25 herein by reference

27. At least since Apple's receipt of notice and/or the filing of the original Complaint on December 21, 2018 (Dkt. 1), Apple has been indirectly infringing, and continues to indirectly infringe, at least claims 11, 18, and 23 of the '125 Patent through its partners' and service operators', including merchants and end-users, direct infringement of at least claims 11, 18, and 23 of the '125 Patent through, at least, use of the Apple Devices that include the Apple infringing embedded technology, without authorization or license from Fintiv. Such partners and service operators include hundreds of banks in the United States. *See* https://support.apple.com/en-us/HT204916 (last visited 4/2/2019).

28. Apple is contributing to the infringement by others and/or inducing infringement by others, by, among other things, providing a mobile wallet that enables the provisioning of contactless cards. Apple has also contributed and/or induced, and continues to contribute and/or induce the infringement of at least claims 11, 18, and 23 of the '125 Patent by contributing to and/or inducing its partners and service operators to use Apple's products, such as the Apple Devices, in an infringing manner as described above, including encouraging and instructing its partners and service operators through software and documentation provided by Apple. For example, Apple's websites specifically instruct and show end-users how to install and manage cards (*e.g.*, debit and credit cards) through Apple Wallet on Apple Devices. *See*, *e.g.*, https://support.apple.com/en-us/HT204506 (last visited 4/8/2019); https://support.apple.com/en-us/HT204003 (last visited 4/8/2019);

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf (last visited 4/8/2019); https://developer.apple.com/wallet/ (last visited 4/2/2019); https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/index.html#//apple_ref/doc/uid/TP40012195 (last visited 4/2/2019).

29. Apple has specifically intended to encourage its partners and service operators use its products that infringe at least claims 11, 18, and 23 of the '125 Patent by, at a minimum, providing access to support, training, tutorials, and instructions, including a video demonstration with a step-by-step guide detailing how to use Apple Wallet, for its infringing products to its partners and service operators to enable them to infringe at least claims 11, 18, and 23 of the '125 Patent, as described above. *See, e.g.,* https://developer.apple.com/videos/play/wwdc2018/720/?time=1347 (last visited 4/2/2019); https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/YourFirst.html#//apple_ref/doc/uid/TP40012195-CH2-SW1 (last visited 4/2/2019).

30. Apple has known, at least as early as the service of the original Complaint, that its infringing products, such as Apple Wallet on Apple Devices, cannot be used without infringing the technology claimed in the '125 Patent, as described above, and are not staple articles of commerce suitable for substantial non-infringing uses. Apple has known, at least as early as the service of the original Complaint, that its infringing products, such as Apple Wallet on Apple Devices, are especially made or adapted for use that results in infringement of the '125 Patent as described above.

31. Fintiv has been damaged by Apple's infringement of the '125 Patent and will continue to be damaged by such infringement. Fintiv is entitled to recover damages from Apple

to compensate it for Apple's infringement, as alleged above, in an amount measured by no less than a reasonable royalty under 35 U.S.C. § 284.

V. DEMAND FOR JURY TRIAL

Fintiv demands a trial by jury of any and all issues triable of right before a jury.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff Fintiv respectfully requests that the Court:

A. Enter a judgment that Apple directly infringes, contributorily infringes, and/or induces infringement of one or more claims of the '125 Patent;

B. Enter a judgment awarding Plaintiff Fintiv all damages adequate to compensate it for Defendant Apple's direct or contributory infringement of, or inducement to infringe, the '125 Patent, including all pre-judgment and post-judgment interest at the maximum rate permitted by law;

C. Declare this case exceptional pursuant to 35 U.S.C. §285; and

D. Award Plaintiff Fintiv its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court.

Dated: April 9, 2019

RESPECTFULLY SUBMITTED,

By: */s/ Jonathan K. Waldrop*

J. Mark Mann (Texas Bar No. 12926150)
mark@themannfirm.com
G. Blake Thompson (Texas Bar No. 24042033)
blake@themannfirm.com
MANN | TINDEL | THOMPSON
300 W. Main Street
Henderson, Texas 75652
913 Franklin Ave., Suite 201
Waco, Texas 76701
Telephone: (903) 657-8540
Facsimile: (903) 657-6003

Andy Tindel (Texas Bar No. 20054500)
atindel@andytindel.com
MANN | TINDEL | THOMPSON
112 E. Line Street, Suite 304
Tyler, Texas 75702
Telephone: (903) 596-0900
Facsimile: (903) 596-0909

Craig D. Cherry (Texas Bar No. 24012419)
ccherry@haleyolson.com
HALEY & OLSON, P.C.
100 N. Ritchie Road, Suite 200
Waco, Texas 76701
Telephone: (254) 776-3336
Facsimile: (254) 776-6823

Jonathan K. Waldrop (CA Bar No. 297903)
(Admitted in this District)
jwaldrop@kasowitz.com
Darcy L. Jones (CA Bar No. 309474)
(Admitted in this District)
djones@kasowitz.com
Marcus A. Barber (CA Bar No. 307361)
(Admitted in this District)
mbarber@kasowitz.com
John W. Downing (CA Bar No. 252850)
(Admitted in this District)
jdowning@kasowitz.com
Heather S. Kim (CA Bar No. 277686)
(Admitted in this District)
hkim@kasowitz.com
Jack Shaw (CA Bar No. 309382)
(Admitted in this District)
jshaw@kasowitz.com
Gurtej Singh (CA Bar No. 286547)
(Admitted in this District)
gsingh@kasowitz.com

KASOWITZ BENSON TORRES LLP
333 Twin Dolphin Drive, Suite 200
Redwood Shores, California 94065
Telephone: (650) 453-5170
Facsimile: (650) 453-5171

Daniel C. Miller (NY Bar No. 4232773)
(*pro hac vice*)
KASOWITZ BENSON TORRES LLP
1399 New York Avenue NW, Suite 201
Washington, DC 20005
Telephone: (202) 760-3400
Facsimile: (202) 760-3401
Email: dcmiller@kasowitz.com

Rodney R. Miller (Texas Bar No. 24070280)
(Admitted in this District)
KASOWITZ BENSON TORRES LLP
1349 West Peachtree Street N.W., Suite 1500
Atlanta, Georgia 30309
Telephone: (404) 260-6080
Facsimile: (404) 260-6081
Email: rmiller@kasowitz.com

Attorneys for Plaintiff
FINTIV, INC.

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via U.S. District Court [LIVE] — Document Filing System, to all counsel of record, on this 9th day of April, 2019.

/s/ Jonathan K. Waldrop
Jonathan K. Waldrop